I applaud CISA for increasing these trainings, which H.R. 7777—which I love saying—would make permanent. This commonsense program is an easy solution to build resilience against cyberattacks for our most vulnerable systems.

Madam Speaker, I urge my House colleagues to support this legislation, and I reserve the balance of my time.

Mrs. MILLER-MEEKS. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 7777, the Industrial Control Systems Cybersecurity Training Act.

In policy discussions following recent cyber incidents, like SolarWinds and Colonial Pipeline, one constant area of concern to Congress and our cyber defenders, like the Cybersecurity and Infrastructure Security Agency, CISA, has been improving the Nation's workforce pipeline for cybersecurity and other STEM-related fields.

As the interconnectivity of our daily lives continues to grow, the estimated worldwide cost of cybercrime has risen to $6 trillion annually. Despite this alarming and growing threat, some estimates say that the cybersecurity workforce is currently short about 1 to 3 million qualified professionals.

A recent Center for Strategic and International Studies, CSIS, study of IT decisionmakers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organization.

□ 1415

Federal agencies have been working to bridge the gap in skills required to prepare a future cyber workforce.

CISA is collaborating closely with organizations like the National Institute of Standards and Technology, NIST, to identify cyber knowledge deficits on a sector-by-sector basis. One example is the National Initiative for Cybersecurity Education framework, which serves as a useful precursor for directing Federal resources into education and research priorities.

H.R. 7777 would require that CISA provide resources for the purpose of training cyber operators that are fluent across multiple segments of the cyber domain, not only information technology but also operational technology, like manufacturing systems and industrial control systems, which are commonplace within critical infrastructure sectors and are increasingly exposed to cyber risk.

We must continue to do all we can to improve our Nation's cyber posture and focus on policy that can help make our government and private sector critical infrastructure operations more resilient and prepared for future events.

Madam Speaker, I urge Members to join me in supporting H.R. 7777, and I yield back the balance of my time.

Mr. SWALWELL. Madam Speaker, I yield myself the balance of my time.

I appreciate the bipartisan, cooperative effort here to make sure that our cyber professionals across America are ready to meet the growing threats from Russia, China, and even nonstate cyber actors. That is exactly what H.R. 7777 seeks to do, by authorizing CISA's ICS cybersecurity training program and directing CISA to report to Congress annually about the initiative.

Improving the state of our cybersecurity workforce will be an ongoing effort, and these reports will help Congress continue to strengthen this program in the future.

Passing this bill will help us continue to move forward in developing the cybersecurity workforce we need to defend against the growing cyber threats that we face. In particular, this will help strengthen small businesses, particularly those in critical infrastructure, who do not yet today have cybersecurity defense forces receiving that training.

Madam Speaker, I urge my colleagues to support H.R. 7777, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. SWALWELL) that the House suspend the rules and pass the bill, H.R. 7777, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ROY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

NATIONAL COMPUTER FORENSICS INSTITUTE REAUTHORIZATION ACT OF 2022

Mr. SWALWELL. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 7174) to amend the Homeland Security Act of 2002 to reauthorize the National Computer Forensics Institute of the United States Secret Service, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7174

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Computer Forensics Institute Reauthorization Act of 2022''.

SEC. 2. REAUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383) is amended—

(1) in subsection (a)—

(A) in the subsection heading, by striking ''IN GENERAL'' and inserting ''IN GENERAL; MISSION'';

(B) by striking ''2022'' and inserting ''2032''; and

(C) by striking the second sentence and inserting ''The Institute's mission shall be to educate, train, and equip State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service's network of cyber fraud task forces, and other appropriate individuals regarding the investigation and prevention of cybersecurity incidents, electronic crimes, and related cybersecurity threats, including through the dissemination of homeland security information, in accordance with relevant Department guidance regarding privacy, civil rights, and civil liberties protections.'';

(2) by redesignating subsections (c) through (f) as subsections (d) through (g), respectively;

(3) by striking subsection (b) and inserting the following new subsections:

''(b) CURRICULUM.—In furtherance of subsection (a), all education and training of the Institute shall be conducted in accordance with relevant Federal law and policy regarding privacy, civil rights, and civil liberties protections, including best practices for safeguarding data privacy and fair information practice principles. Education and training provided pursuant to subsection (a) shall relate to the following:

''(1) Investigating and preventing cybersecurity incidents, electronic crimes, and related cybersecurity threats, including relating to instances involving illicit use of digital assets and emerging trends in cybersecurity and electronic crime.

''(2) Conducting forensic examinations of computers, mobile devices, and other information systems.

''(3) Prosecutorial and judicial considerations related to cybersecurity incidents, electronic crimes, related cybersecurity threats, and forensic examinations of computers, mobile devices, and other information systems.

''(4) Methods to obtain, process, store, and admit digital evidence in court.

''(c) RESEARCH AND DEVELOPMENT.—In furtherance of subsection (a), the Institute shall research, develop, and share information relating to investigating cybersecurity incidents, electronic crimes, and related cybersecurity threats that prioritize best practices for forensic examinations of computers, mobile devices, and other information systems. Such information may include training on methods to investigate ransomware and other threats involving the use of digital assets.'';

(4) in subsection (d), as so redesignated—

(A) by striking ''cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers and prosecutors'' and inserting ''cybersecurity incidents, electronic crimes, and related cybersecurity threats is shared with recipients of education and training provided pursuant to subsection (a)''; and

(B) by adding at the end the following new sentence: ''The Institute shall prioritize providing education and training to individuals from geographically-diverse jurisdictions throughout the United States.'';

(5) in subsection (e), as so redesignated—

(A) by striking ''State, local, tribal, and territorial law enforcement officers'' and inserting ''recipients of education and training provided pursuant to subsection (a)''; and

(B) by striking ''necessary to conduct cyber and electronic crime and related threat investigations and computer and mobile device forensic examinations'' and inserting ''for investigating and preventing cybersecurity incidents, electronic crimes, related cybersecurity threats, and for forensic examinations of computers, mobile devices, and other information systems'';

(6) in subsection (f), as so redesignated—

(A) by amending the heading to read as follows: ''CYBER FRAUD TASK FORCES'';

(B) by striking ''Electronic Crime'' and inserting ''Cyber Fraud'';

(C) by striking ''State, local, tribal, and territorial law enforcement officers'' and inserting

''recipients of education and training provided pursuant to subsection (a)''; and

(D) by striking ''at'' and inserting ''by'';

(7) by redesignating subsection (g), as redesignated pursuant to paragraph (2), as subsection (j); and

(8) by inserting after subsection (f), as so redesignated, the following new subsections:

''(g) EXPENSES.—The Director of the United States Secret Service may pay for all or a part of the education, training, or equipment provided by the Institute, including relating to the travel, transportation, and subsistence expenses of recipients of education and training provided pursuant to subsection (a).

''(h) ANNUAL REPORTS TO CONGRESS.—The Secretary shall include in the annual report required pursuant to section 1116 of title 31, United States Code, information regarding the activities of the Institute, including relating to the following:

''(1) Activities of the Institute, including, where possible, an identification of jurisdictions with recipients of education and training provided pursuant to subsection (a) of this section during such year and information relating to the costs associated with such education and training.

''(2) Any information regarding projected future demand for such education and training.

''(3) Impacts of the Institute's activities on jurisdictions' capability to investigate and prevent cybersecurity incidents, electronic crimes, and related cybersecurity threats.

''(4) A description of the nomination process for State, local, territorial, and Tribal law enforcement officers, prosecutors, judges, participants in the United States Secret Service's network of cyber fraud task forces, and other appropriate individuals to receive the education and training provided pursuant to subsection (a).

''(5) Any other issues determined relevant by the Secretary.

''(i) DEFINITIONS.—In this section—

''(1) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501))

''(2) INCIDENT.—The term 'incident' has the meaning given such term in section 2209(a).

''(3) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))).''.

(b) GUIDANCE FROM THE PRIVACY OFFICER AND CIVIL RIGHTS AND CIVIL LIBERTIES OFFICER.—The Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall provide guidance, upon the request of the Director of the United States Secret Service, regarding the functions specified in subsection (b) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(c) TEMPLATE FOR INFORMATION COLLECTION FROM PARTICIPATING JURISDICTIONS.—Not later than 180 days after the date of the enactment of this Act, the Director of the United States Secret Service shall develop and disseminate to jurisdictions that are recipients of education and training provided by the National Computer Forensics Institute pursuant to subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a), a template to permit each such jurisdiction to submit to the Director reports on the impacts on such jurisdiction of such education and training, including information on the number of digital forensics exams conducted annually. The Director shall, as appropriate, revise such template and disseminate to jurisdictions described in this subsection any such revised templates.

(d) REQUIREMENTS ANALYSIS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director of the United States Secret Service shall carry out a requirements analysis of approaches to expand capacity of the National Computer Forensics Institute to carry out the Institute's mission as set forth in subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

(2) SUBMISSION.—Not later than 90 days after completing the requirements analysis under paragraph (1), the Director of the United States Secret Service shall submit to Congress such analysis, together with a plan to expand the capacity of the National Computer Forensics Institute to provide education and training described in such subsection. Such analysis and plan shall consider the following:

(A) Expanding the physical operations of the Institute.

(B) Expanding the availability of virtual education and training to all or a subset of potential recipients of education and training from the Institute.

(C) Some combination of the considerations set forth in subparagraphs (A) and (B).

(e) RESEARCH AND DEVELOPMENT.—The Director of the United States Secret Service may coordinate with the Under Secretary for Science and Technology of the Department of Homeland Security to carry out research and development of systems and procedures to enhance the National Computer Forensics Institute's capabilities and capacity to carry out the Institute's mission as set forth in subsection (a) of section 822 of the Homeland Security Act of 2002 (6 U.S.C. 383), as amended by subsection (a).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. SWALWELL) and the gentlewoman from Iowa (Mrs. MILLER-MEEKS) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. SWALWELL. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from California?

There was no objection.

Mr. SWALWELL. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 7174, the National Computer Forensics Institute Reauthorization Act of 2022, introduced in this House by Ms. SLOTKIN of Michigan.

Ms. SLOTKIN's legislation addresses ransomware threats that are on the rise and are costing American companies and the American people millions of dollars each year. In fact, former Cisco CEO John Chambers estimates that in the year 2022, we will see approximately $120,000, on average, in costs to 60,000 American businesses who will be victims of ransomware attacks.

Ransomware attacks have targeted our most critical industries, from the energy sector to food processing to schools and even hospitals. State and local law enforcement are on the front lines of protecting against this threat and often are the first people called when an attack occurs, and they are on the ground in communities to respond.

Recently, FBI Director Chris Wray told Congress that within an hour, if a business calls the FBI, one of his agents can respond, either virtually or at their doorstep, to assist them.

More than ever, State and local law enforcement need the training and tools to investigate and respond to ransomware and other cyber-based attacks. That is where the National Computer Forensics Institute, or NCFI, comes in.

Established in 2008 by the U.S. Secret Service, NCFI is recognized as a preeminent Federal facility for State and local law enforcement to receive cybersecurity training.

At NCFI, the Secret Service trains State, local, Tribal, and territory officers, prosecutors, and judges in cybercrime investigations and cyber-incident response.

To date, because of this training, more than 18,000 law enforcement officers, prosecutors, and judges across all 50 States and territories have received training at NCFI's center in Hoover, Alabama.

As introduced, Ms. SLOTKIN's H.R. 7174 would reauthorize NCFI through 2032.

Like many of my colleagues here in Congress, I began my career as a prosecutor, and I know the importance of training law enforcement, prosecutors, and judicial officers.

Before a case ever reaches the trial stage, dozens of law enforcement officers, investigators, and attorneys have pored over every shred of evidence to ensure justice is served.

Since evidence today is increasingly digital and more and more meticulous to review, it is imperative that law enforcement, prosecutors, and judicial officers from communities across the country have access to necessary training on emerging and digital technologies, like AI, and equipment to put that training into action. That is what Ms. SLOTKIN's bill will do.

H.R. 7174 will ensure that NCFI's operation will continue for 10 more years and better position the institute for success.

The bill strengthens its operations by requiring privacy, civil rights, and civil liberties protections be integrated into the training; it authorizes NCFI to engage in research and development of different approaches to training for investigations involving ransomware and threats involving the use of emerging digital assets; and it requires the Secret Service Director to report on the demand for training at NCFI, the institute's ability to meet that demand, and whether to expand further NCFI facilities and training opportunities.

NCFI's authority to continue its training will end in November of this year, but we know that cyber actors, nation-state and non-nation-state, their efforts will not, which makes H.R. 7174's swift passage so important.

The House authorized the NCFI by an overwhelming bipartisan vote in the 115th Congress, and the Committee on

Homeland Security passed this bipartisan bill by unanimous voice vote last month. It has 17 bipartisan cosponsors.

Madam Speaker, I urge my colleague to support Ms. SLOTKIN's legislation once again, and I reserve the balance of my time.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, June 8, 2022.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security, House of Representatives, Washington, DC.

DEAR CHAIRMAN THOMPSON: This letter is to advise you that the Committee on the Judiciary has now had an opportunity to review the provisions in H.R. 7174, the ''National Computer Forensics Institute Reauthorization Act of 2022,'' that fall within our Rule X jurisdiction. I appreciate your consulting with us on those provisions. The Judiciary Committee has no objection to your including them in the bill for consideration on the House floor, and to expedite that consideration is willing to forgo action on H.R. 7174, with the understanding that we do not thereby waive any future jurisdictional claim over those provisions or their subject matters.

In the event a House-Senate conference on this or similar legislation is convened, the Judiciary Committee reserves the right to request an appropriate number of conferees to address any concerns with these or similar provisions that may arise in conference.

Please place this letter into the Congressional Record during consideration of the measure on the House floor. Thank you for the cooperative spirit in which you have worked regarding this matter and others between our committees.

Sincerely,

JERROLD NADLER,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, June 8, 2022.

Hon. JERROLD NADLER,
Chairman, Committee on the Judiciary, House of Representatives, Washington, DC.

DEAR CHAIRMAN NADLER: Thank you for your letter regarding H.R. 7174, the ''National Computer Forensics Institute Reauthorization Act of 2022.'' I recognize that the Committee on the Judiciary has a jurisdictional interest in H.R. 7174, and I appreciate your effort to allow this bill to be considered on the House floor.

I concur with you that forgoing action on the bill does not in any way prejudice the Committee on the Judiciary with respect to its jurisdictional prerogatives on this bill or similar legislation in the future, and I would support your effort to seek appointment of an appropriate number of conferees to any House-Senate conference involving this legislation.

I will include our letters on H.R. 7174 in the Committee report on this measure and in the Congressional Record during floor consideration of this bill. I look forward to working with you on this legislation and other matters of great importance to this Nation.

Sincerely,

BENNIE G. THOMPSON,
Chairman,
Committee on Homeland Security.

Mrs. MILLER-MEEKS. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 7174, the National Computer Forensics Institute Reauthorization Act.

Our Nation is facing an increase in cyber threats stemming from multiple angles. These range from critical infrastructure vulnerabilities to child exploitation online.

Previous cyberattacks have highlighted the need for preventive measures and law enforcement support at every level, including Federal, State, local, Tribal, and territorial.

Many recent attacks and exploited vulnerabilities have severely impacted the American people and economy. Adding to this, with the ongoing war in Ukraine, the intelligence community is warning of a heightened cyber threat from Russia.

The National Computer Forensics Institute in Hoover, Alabama, is operated by the United States Secret Service. NCFI provides essential education and training to State, local, Tribal, and territorial law enforcement, prosecutors, and judges on how to mitigate, detect, and respond to cyber threats.

Since opening in 2008, NCFI has continuously worked to equip its students with the necessary tools and knowledge needed to prevent cybercrime.

Now, more than ever, as we are facing cyberattacks from malicious actors like Russia, China, and Iran, in addition to other criminal behavior online like child pornography, bolstering cyber training and tools for our law enforcement partners is imperative.

Congress officially authorized the NCFI for 5 years in 2017. This bill reauthorizes NCFI for 10 years and updates its mission, function, and curriculum.

In addition, the bill requires an annual report on NCFI's impact and activities, a requirements analysis for its potential expansion, and a process to receive feedback from participating jurisdictions.

Cybersecurity has never been more important to homeland security, and it is pivotal that we train our State and local law enforcement to address this threat and other online nefarious activities head-on.

Madam Speaker, I urge Members to join me in supporting H.R. 7174, and I yield back the balance of my time.

Mr. SWALWELL. Madam Speaker, I yield myself the balance of my time.

As stated, the NCFI training and education program is too important to expire. It will do so in November. I appreciate the gentlewoman from Iowa and her side's support for this legislation.

Madam Speaker, I urge swift passage of H.R. 7174, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from California (Mr. SWALWELL) that the House suspend the rules and pass the bill, H.R. 7174, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ROY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

PREVENT EXPOSURE TO NARCOTICS AND TOXICS ACT OF 2021

Mr. SWALWELL. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 5274) to amend the Homeland Security Act of 2002 to provide training for U.S. Customs and Border Protection personnel on the use of containment devices to prevent secondary exposure to fentanyl and other potentially lethal substances, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5274

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Prevent Exposure to Narcotics and Toxics Act of 2021'' or the ''PREVENT ACT of 2021''.

SEC. 2. PROVIDING TRAINING FOR U.S. CUSTOMS AND BORDER PROTECTION PERSONNEL ON THE USE OF CONTAINMENT DEVICES TO PREVENT SECONDARY EXPOSURE TO FENTANYL AND OTHER POTENTIALLY LETHAL SUBSTANCES.

(a) TRAINING.—Paragraph (1) of section 416(b) of the Homeland Security Act of 2002 (6 U.S.C. 216(b)) is amended by adding at the end the following new subparagraph:

''(C) How to use containment devices to prevent secondary exposure to fentanyl and other potentially lethal substances.''.

(b) AVAILABILITY OF CONTAINMENT DEVICES.—Section 416(c) of the Homeland Security Act of 2002 (6 U.S.C. 216(c)) is amended—

(1) by striking ''and'' after ''equipment'' and inserting a comma; and

(2) by inserting ''and containment devices'' after ''naloxone,''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. SWALWELL) and the gentlewoman from Iowa (Mrs. MILLER-MEEKS) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. SWALWELL. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from California?

There was no objection.

Mr. SWALWELL. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 5274, the Prevent Exposure to Narcotics and Toxics Act, as introduced by my friend and colleague, Representative JOYCE of Ohio. I see that he is here, so I will let him speak on his bill, and I will follow up shortly.

I urge my colleagues to support this bill, and I reserve the balance of my time.